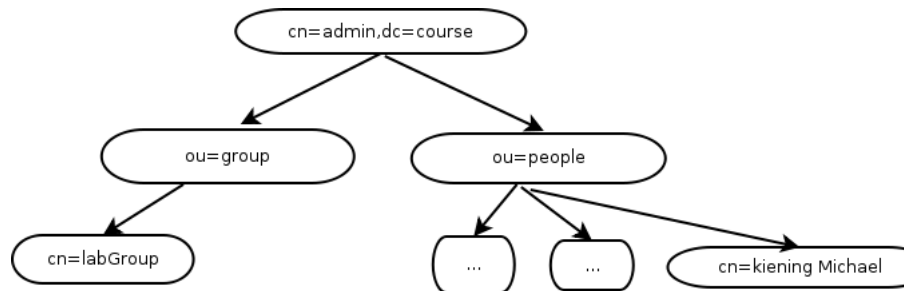


LDAP - Light Weight Access Protocol

Michael Kiening

June 6, 2011



cn: common name

ou: organizational units

dc: domain component

goal

The goal: have regular users' accounts maintained in the LDAP directory
tasks:

- ▶ install missing packages: `nscd`, `libnss-ldap`, `ldap-utils`, `slapd`
- ▶ manage root account for `slapd`
- ▶ add 2 organizational units:
 - ▶ `ou=people,dc=course`
 - ▶ `ou=group,dc=course`
- ▶ add your group as an 'objectClass: `posixGroup`':
`cn=<usr>,ou=group,dc=course`
- ▶ add your user as an 'objectClass: `posixAccount`; objectClass `shadowAccount`; objectClass `inetOrgPerson`':
`uid=<usr>,ou=people,dc=course`
- ▶ adjust name service switch
- ▶ delete old userentries and login to virtual machine using `ldap` account

install missing packages and set up root account

```
$: aptitude install nscd,libnss-ldap ldap-utils slapd
```

```
$: dpkg-reconfigure slapd
```

- ▶ Omit OpenLDAP server configuration? \Rightarrow no
- ▶ DNS domain \Rightarrow course
- ▶ organization name \Rightarrow course
- ▶ Administrator password \Rightarrow choosePW
- ▶ confirm password \Rightarrow confirm chosen PW
- ▶ Database backend to use \Rightarrow HDB
- ▶ Do you want the database to be removed when slapd is purged? \Rightarrow no
- ▶ Allow LDAPv2 protocol? \Rightarrow no

set up password for the root account

\$: slappasswd → enter PW

→ reenter PW

⇒ SSHAMre45tuMwwrx4XY118/19BJMAqjLG01n

\$: vim /etc/ldap/slapd.d/cn=config/olcDatabase=0config.ldif

dn: olcDatabase=0config

objectClass: olcDatabaseConfig

olcDatabase: 0config

olcAccess: 0to * by

dn.exact=gidNumber=0+uidNumber=0,cn=peercred,cn=external
,cn=auth manage by * break

olcRootDN: cn=admin,cn=config

olcRootPW: {SSHA}Mre45tuMwwrx4XY118/19BJMAqjLG01n

add users, groups and units

```
$: ldapvi -discover -D cn=admin,dc=course -h ldapi:///'
```

```
add organizational unit people as child of dc=course:
```

```
add ou=people,dc=course
```

```
objectClass: organizationalUnit
```

```
ou: people
```

```
add organizational unit labGroup as child of dc=course
```

```
add cn=labGroup,ou=group,dc=course
```

```
objectClass: posixGroup
```

```
cn: labGroup
```

```
gidNumber: 1014
```

add users, groups and units

add user as child of people, and member of labGroup

add uid=kiening,ou=people,dc=course

objectClass: posixAccount

objectClass: shadowAccount

objectClass: inetOrgPerson

shadowLastChange: 1

uid: kiening

cn: kiening

gidNumber: 1014

homeDirectory: /home/kiening

sn: Kiening

uidNumber: 1014

userPassword: SSHAx6EkGLcJCWFu3/O+J0ifwTEh+2VSDUL

adjust nsswitch for ldap

```
$: vim /etc/nsswitch.conf
```

```
# /etc/nsswitch.conf
```

```
#
```

```
# Example configuration of GNU Name Service Switch  
functionality.
```

```
# If you have the 'glibc-doc-reference' and 'info' packages  
installed, try:
```

```
# 'info libc "Name Service Switch"' for information about this file.
```

```
passwd: compat ldap
```

```
group: compat ldap
```

```
shadow: compat ldap
```

```
hosts: files dns
```

```
networks: files
```

```
protocols: db files
```

```
services: db files
```

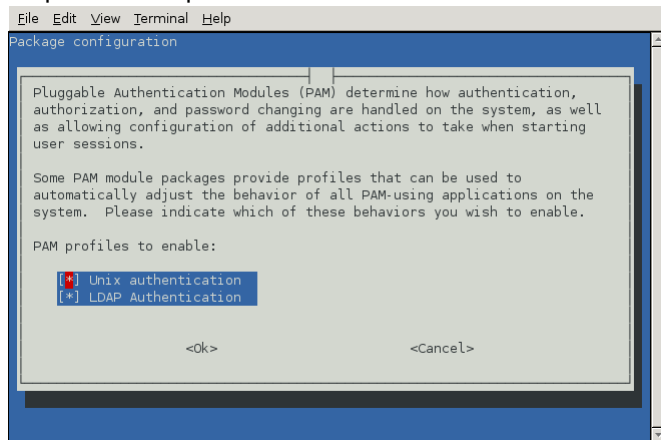
```
ethers: db files
```

```
rpc: db files
```

```
netgroup: nis
```


enable Idap for PAM

\$: pam-auth-update



delete common user and login via ldap

check using `getent passwd` and `getent group` if user and group are listed.

(twice, once ldap entry and once common user)

delete user and group entries in

- ▶ `/etc/passwd`
- ▶ `/etc/groups`
- ▶ `/etc/shadow`
- ▶ `/etc/gshadow`

relog into virtual machine using `ldap-user`.

Thank you for your attention!